Editor's Comments: Welcome to The Journal of Physical Security

> He that will not apply new remedies must expect new evils; for time is the greatest innovator.
>
> -- Francis Bacon (1561-1626)

> Security can only be achieved through constant change, through discarding old ideas that have outlived their usefulness and adapting others to current facts.
>
> -- William O. Douglas (1898-1980)

> In theory there is no difference between theory and practice. In practice there is.
>
> -- Yogi Berra

Physical security is about protecting valuable, tangible assets from harm. The "assets" can include, inter alia, people, buildings, equipment, materials, chemicals, hazardous waste, documents, products, merchandise, food & drink, drugs, weapons, money, and museum artifacts. The "harm" that we wish to avoid might involve theft, destruction, sabotage, vandalism, terrorism, espionage, counterfeiting, tampering, or unauthorized access.

It is clear that modern physical security has myriad problems. It suffers from a serious lack of identity, efficacy, innovation, rigor, integrity, metrics, standards, peer-review, theories/models/paradigms, and a "scientific" or academic footing. It often fails to be sufficiently holistic, predictive, preventative, and multi-disciplinary. Physical security practitioners are rarely effective in combining the social sciences with the technical sciences. The horrific terrorist attacks of September 11, 2001 only serve to further highlight some of these shortcomings.

This new journal is a modest effort to deal with some of the serious problems with the field of physical security—in particular, the lack of scholarly peer-reviewed journals. There are a number of useful trade journals that cover physical security. There are also numerous peer-review journals that focus on criminology, law enforcement, cryptography, terrorism, national security, computer security, or security management. The field of physical security, however, has long needed a journal that can serve as a central focus, as well as

a vehicle for rigorous discussion and advancement of the field, especially in the areas of research, development, modeling, testing, and analysis.

What are some of the other problems with the field of physical security? Well, for one thing, it is scarcely a "field" at all. Despite the past, present, and future importance of physical security, it is very difficult to get a formal degree in physical security from a major U.S. university. (A degree in criminology or computer security is about as close as one can usually come.) There are remarkably few introductory or advanced textbooks covering major areas of physical security, such as tamper detection, access control, and biometrics. There are some useful introductory survey textbooks about physical security in general, but few that operate at a very sophisticated level. Despite the fact that physical security is becoming increasingly high-tech, there are almost no national or international conferences where research and development results regarding physical security can be presented. Most conferences that cover physical security emphasize lectures by (often self-identified) security experts who tell war stories or espouse simplistic solutions and platitudes. Platitudes are a particularly annoying scourge for physical security—along with other unsavory elements borrowed from modern Management Science. For a variety of reasons (including that it doesn't seem to fit anywhere else), physical security is often viewed as a pseudo-subfield of management.

Physical security is also problematic because it is so difficult. Recognition of this fact is essential because complacency, overconfidence, and arrogance are incompatible with good security. One of the reasons that physical security is such a daunting task is that it is highly multidimensional. Whereas an adversary need only find and exploit one or a small number of vulnerabilities to succeed, physical security managers must identify, understand, and manage all possible vulnerabilities. While adversaries can attack at only one or a small number of points, security managers must often protect large, spatially distributed facilities. They must plan for all possible attacks at unpredictable times from all possible adversaries, many of whom may be completely unknown. Whereas security personnel are generally constrained by legal, ethical, humane, organizational, and public relations considerations, their adversaries (e.g., terrorists) may not be.

Another serious challenge for physical security is the general lack of useful performance measures. The traditional performance measure for security is pathological: success is defined as nothing happening. This kind of performance measure does not permit effective cost/benefit analysis, and

often results in insufficient resources being made available for security. Moreover, it tends to result in irrational cyclical fluctuations in security funding. Security budgets typically decay over time as long as there are no major security incidents. Once a major incident occurs, however, hysteria tends to ensue. Massive resources are suddenly thrown at the problem, much of them ultimately wasted. Draconian and often downright silly measures are introduced, some of which actually decrease overall security, or at least divert attention and resources from more effective measures. (Thus, for example, we saw airport screeners after September 11th confiscating fingernail clippers from airline passengers—presumably to keep would-be terrorists from threatening the pilots with bad manicures.) Once a security crisis passes, the emphasis on physical security typically again erodes away until the next serious incident, at which point another frantic spike in funding and activity occurs.

Effective physical security is also hampered by a lack of standards. The few standards that do exist are of little value. Standards, however, are not automatically a guarantee of effective security. If they are too broad or too narrow, not well thought through, and/or mindlessly applied, they can cause more harm than good. Moreover, there is the potential problem referred to in the old engineering joke: that the great thing about standards is that there are so many to choose from!

Physical security is also commonly plagued by ambiguity. Security programs are frequently quite vague as to exact goals and adversaries. Not helping the problem is the fact that security terminology is often sloppy, misleading, misunderstood, or misused, even by experienced security professionals.

Attitude can be a particularly significant problem for a physical security program. While there are potential benefits to showing great confidence to the outside world (because this may discourage adversaries), a healthy security program does not believe its own public guarantees and assurances. Far too often, however, physical security managers, and the high-level personnel they report to, believe their own press releases. Even worse, many security programs retaliate against insiders or outsiders who question security measures, identify vulnerabilities, offer suggestions, or call for improvements. The idea of genuine “peer review” is a largely alien concept to the field of physical security, either for the practice of security, or for research, development, and testing.

The field also suffers from society’s ambivalent attitudes towards security,

often involving the inevitable conflict between liberty and security. Other challenges include the multidisciplinary and (increasingly) technological nature of physical security, the relatively low status and educational level of many security practitioners, the boredom often associated with routine security functions, and the tendency for the field to attract the wrong type of people. Indeed, the field of physical security seems to have more than its fair share of linear, concrete, and wishful thinkers, as well as control freaks, knuckleheads, egotists, charlatans, washouts, socially maladjusted loners, bureaucrats, and those skilled at self-deception. Ironically, physical security actually requires some of the most sophisticated and diverse of all possible abilities: good observational skills, a subtle understanding of human psychology, respect for civil liberties, awareness of complex legal issues, sound judgment when working in gray areas, the ability to plan effectively but also to think and react quickly on one's own initiative, engineering sophistication, and considerable imagination and creativity in order to foresee threats. To make matters worse, people and funding are nowadays drawn more towards digital security (computers, software, networks, and the Internet) than to physical security—even though physical security is in many ways far more critical to both society and the economy than digital security.

"Compliance mode" can also be a major problem. This involves security managers or other security personnel being so focused on satisfying superiors, auditors, regulators, bureaucrats, and formal security requirements that they lose sight of real-world security threats. Being distracted by paperwork and busywork is a serious problem with physical security which, first and foremost, needs to be about paying attention. Compliance mode is very difficult to avoid in large organizations and bureaucracies, in well-established operations, and for security programs that do not encourage security personnel to be flexible, creative, introspective, clever, and proactive (and that do not have senior officials with these attributes).

Further supporting the suspicion that physical security is not a serious or mature field is the behavior of vendors and manufacturers of physical security products. Far too many make "snake oil" claims that are blatantly inaccurate, misleading, naive, or ludicrous. This is especially the case in the areas of tamper detection, access control, and biometrics. Even the most outrageous claims are rarely challenged.

This Journal will not solve all these problems. We can hope, however, to contribute to the advancement and understanding of the field. Physical

security is not just of great practical importance, it is also an intellectually challenging, multidisciplinary, fascinating subject worthy of thoughtful study.

Roger G. Johnston